SYSTEM AND METHOD OF COUNTERACTING UNAUTHORIZED ACCESS TO MICROPHONE DATA

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims benefit of priority under 35 U.S.C. 119(a)-(d) to a Russian Application No. 2016116000 filed on Apr. 25, 2016, which is incorporated by reference herein.

FIELD OF TECHNOLOGY

The disclosure herein generally relates to the protection against loss of data, and more particularly, to systems and methods of counteracting unauthorized access to microphone data.

BACKGROUND

In the modern world, users encounter many cyber threats, one of which is unauthorized access to the user's microphone for the purpose of eavesdropping. In order to realize a control of access to the microphone data on the part of processes running on the user's computer it is necessary to perform a filtration of certain requests within the operating system or obtain access to the context of the request data for identification of the processes requesting access, in order to block those processes for which access has not been authorized. In the Windows XP and older operating systems, this functionality has been resolved by means of intercepting traffic in the region of the "KSmixer.sys" kernel component (the Windows Kernel Streaming technology). Requests to read microphone data in the framework of the traffic being intercepted have gone through a special filter in the context of the process reading the microphone data.

With the advent of Windows Vista, a new architecture WASAPI was developed, consisting of many kernel components and a user mode where the Windows Kernel Streaming technology has remained in the "basic variant", while all of the audio traffic has been put through private COM interfaces of new audio drivers, which are registered on the port driver "portcls.sys". These audio drivers can be realized such that the audio traffic with the help of a Direct Access Memory (DMA) controller ends up at once in the user mode buffer, that is, without the involvement of the processor or any supplemental code. And this buffer is mapped into a protected process "audiodg.exe", from which the data is copied with the help of the processor into the buffer of the user process in the context of this same process "audiodg.exe". That is, the controlling filter in the Windows Kernel Streaming technology has become absolutely unsuitable, starting with Windows Vista.

Due to the foregoing, the need arises for a method which is able to intercept audio traffic from microphones linked to the context of the processes reading the data from the microphones in order to protect transmission of audio data.

SUMMARY

Disclosed are systems, methods and computer program products for counteracting unauthorized access to audio data by transmission of audio data from a microphone to processes.

According to one exemplary aspect, a method is disclosed for preventing unauthorized access to audio data. In this aspect, the method includes storing, in a data buffer by an audiodg.exe process, audio data received from an audio endpoint device; installing, in memory of a computer, a software driver associated with the audio session, the software driver being configured to prevent access to the audio data by unauthorized software applications; receiving, by a processor of the computer, process identifier data from a software application requesting to access the audio data stored in the data buffer; determining, by the processor, whether the application requesting access to the audio data is an unauthorized software application; and controlling, by the processor, the software driver to prevent access to the audio data by the determined unauthorized software application.

According to another exemplary aspect, the method includes converting, by the software driver, the audio data to zeroes when the application requesting access to the audio data is determined to be an unauthorized software application.

According to another exemplary aspect, the method includes monitoring for and intercepting, by the processor, requests from the software application to access the audio data stored in the data buffer.

According to another exemplary aspect, the determining of whether the application requesting access to the audio data is an unauthorized software application comprises at least one of monitoring activities of the requesting application to determine whether the application is trusted or not trusted; scanning the requesting application by accessing a database of signatures of known viruses and comparing a signature of the requesting application; and receiving, from a user, a command whether to grant access to the audio data by the requesting application.

According to another exemplary aspect, the method includes directly storing the audio data received from the audio endpoint device in the data buffer; and only granting access to the audio data by the software driver.

According to another exemplary aspect, the method includes instructing the software driver to grant access to the audio data if the application requesting access to the audio data is an authorized software application; processing, by the software driver, the audio data as an audio stream; and transmitting, by the software driver, the audio data to the determined authorized software application.

According to another exemplary aspect, the method includes installing, in the memory, a plurality of software drivers associated respectively with a plurality of audio streams of the audio session, the software drivers being configured to prevent access to the audio streams, respectively, by unauthorized software applications; receiving, by the processor, process identifier data from at least one software application requesting to access one of the plurality of audio streams; determining, by the processor, whether the at least one application requesting access to the audio stream is an unauthorized software application; and controlling, by the processor, the respective software driver to prevent access to the audio stream by the determined unauthorized software application.

According to another exemplary aspect, a system is disclosed for preventing unauthorized access to audio data. In this aspect, the system includes a data buffer; memory; and a processor configured to: store, in the data buffer by an audiodg.exe process, audio data received from an audio endpoint device, install, in the memory, a software driver associated with the audio session, the software driver being configured to prevent access to the audio data by unauthorized software applications; receive process identifier data from a software application requesting to access the audio